UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ANYWHERECOMMERCE, INC. and BBPOS LIMITED, **Plaintiffs,** **v.** **INGENICO INC., INGENICO CORP., and INGENICO GROUP SA,** **Defendants.**	**Civil Docket No: 1:19-cv-11457-IT**

MEMORANDUM OF LAW IN SUPPORT OF
PLAINTIFFS' MOTION TO COMPEL PRODUCTION OF DOCUMENTS

French data privacy laws have no place in U.S. litigation. The federal courts have agreed – and for good reasons. First, whereas the French General Data Protection Regulation ("French GDPR," as adopted from the European Union's General Data Protection Regulation ("GDPR")) broadly prohibits the transfer of an individual's personal data without that individual's consent, it exempts all transfers that are "necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure" (the "Litigation Exemption"). Plaintiffs requested documents that are necessary for the establishment, exercise, or defense of legal claims, and therefore are entitled to receive them without application of the GDPR's restrictions.

Second, setting aside the Litigation Exemption, the GDPR still should not apply here. Plaintiffs filed their lawsuit in United States federal court, which is governed by the Federal Rules of Civil Procedure. *See* F.R.C.P. 1 (The Federal Rules of Civil Procedure "govern the procedure in all civil actions and proceedings in the United States district courts."). The federal rules grant litigants broad rights to discovery with sufficient protections for confidential and privileged

information. By contrast, the GDPR (and French law generally) is far more restrictive. However, it is well established that foreign laws, such as the GDPR, do not necessarily apply to U.S. litigation simply because a party is based in that foreign country. Rather, courts routinely reject the application the GDPR and other similar laws and, instead, uphold the tenets of American-style discovery.

The Court should do the same here. Plaintiffs have a strong interest in obtaining the documents necessary to prove their claim, without the redaction of every bit of personal identifying information and without having to wait many months for the redactions to be completed. The sought after documents simply are standard business records, not ones targeting any type of confidential personal information. Moreover, the Court has entered a protective order, which provides adequate protection for any type of confidential information. Accordingly, Plaintiffs' interests in efficient and complete discovery outweigh any of Defendants' concerns.

Therefore, the Court should rule that the GDPR does not apply in this litigation.[1]

I. BACKGROUND

A. Facts and Procedural History

Plaintiff AnywhereCommerce, Inc. ("AnywhereCommerce") is in the credit card processing business. It was the first technology company to develop and market a mobile payment "dongle" that connects to the audio port of a wireless device (e.g., smartphone, tablet). Plaintiff BBPOS is a mobile point of sales solution provider, a leading innovator, designer, and

[1] Defendants have noted that Plaintiff BBPOS Limited ("BBPOS") is based in Hong Kong, which too has data privacy laws. However, Plaintiffs believe that those laws do not apply to this litigation because they too have a litigation exception and otherwise should not displace the discovery practice established under the federal rules. In any event, Defendants have no basis to request that the Court apply the Hong Kong restrictions because Defendants are not residents of Hong Kong, do not store any data in Hong Kong, will not be transferring any data from Hong Kong, are not bound by the laws of Hong Kong, and are not intended as protected parties under the Hong Kong laws. Rather, Defendants' only purpose for requesting the application of Hong Kong law would be to increase the burden and cost on BBPOS and to delay the litigation.

manufacturer of end-to-end mobile point of sale solutions, and manufactures mobile point of sale terminals for AnywhereCommerce and others. Through the Plaintiffs' joint efforts, AnywhereCommerce has cornered the market by obtaining all patents related to mobile payment transactions done on smartphones and tablets.

But that did not stop Defendants from developing and selling their own products using Plaintiffs' technology. Defendants are entities affiliated with the Ingenico trade name (collectively, "Ingenico"), which has been a significant manufacturer and seller of card-based electronic point of sale payment terminals. Its focus had been on in-store and online electronic payments – not mobile payments, the space occupied by Plaintiffs.

That changed in or around 2009, when Ingenico acquired ROAM Data, Inc. ("ROAM"), a U.S.-based mobile point of sale device supplier (and direct competitor of Plaintiffs) that had obtained a license from Plaintiffs to use their patented technology. By acquiring ROAM, Ingenico gained access to Plaintiffs' trade secrets and wrongfully misappropriated those trade secrets by using them to develop its own product line. At the same time, Ingenico also showed interest in acquiring each of AnywhereCommerce and BBPOS. Based on that alleged interest, Ingenico requested and received Plaintiffs' trade secrets. That information was provided solely for purposes of evaluating a potential acquisition, but instead, Ingenico used the secret information to develop the same technology and compete for Plaintiffs' business.

Ingenico made its pivotal move in 2014 when it submitted a bid for a lucrative mobile point of sale technology contract with First Data Corporation ("First Data"), with whom Plaintiffs had maintained a long-standing business relationship. Indeed, Plaintiffs too had submitted a bid for the same contract. But despite Plaintiffs' history with First Data and their more competitive pricing, First Data awarded the contract to Ingenico. This took a significant economic toll on

Plaintiffs and the losses have continued in the years since, as Ingenico has continued to market is stolen technology. Had it not been for Ingenico's trade secret theft, Plaintiffs would have secured the First Data contract and generated additional business.

In order to recover the losses resulting from Ingenico's wrongful conduct, Plaintiffs filed a civil action asserting claims of (1) tortious interference with existing and prospective contracts and business relationships; (2) violation of the Georgia Trade Secrets Act; (3) violation of the Massachusetts Trade Secret Act; (4) violation of the U.S. Defend Trade Secrets Act of 2016; (5) breach of contract; (6) violation of section 43(a) of the Lanham Act; (7) unjust enrichment; (8) violation of the Georgia Deceptive Trade Practices Act; and (9) violation of the Georgia Fair Business Practices Act. On December 20, 2019, Plaintiffs served their First Set of Requests for Production of Documents Upon Defendants (the "Requests"). (A true and correct copy of the Requests is attached as Exhibit A). But, over three months later, Defendants still have not produced a single document.

B. The GDPR

Part of the alleged holdup has been a concern raised by Defendants as to the possible applicability of the GDPR to discovery in this case (though, as counsel for Defendants admitted during the March 30, 2020 conference, the GDPR issue did not, and does not, prevent Defendants from producing non-ESI documents, including ones that had been identified in initial disclosures many months ago). Defendant Ingenico Group SA – the parent entity of the other Defendants Ingenico Inc. and Ingenico Corp. – is based in France, which, on June 30, 2018, enacted Law n^{o}2018-493, thereby incorporating the GDPR (which had taken effect on May 25, 2018 in all European Union member states) into its existing data protection laws. As is relevant here, the GDPR and French GDPR are identical and the terms may be used interchangeably based on the context.

Under the GDPR, subject to certain exceptions, "personal data" may not be "processed" without the "data subject's" "consent." (Exhibit B, GDPR, Article 6(1)). These terms are defined as follows:

- "'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction";

- "'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person";

- "'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her";

(*Id.*, Article 4). If applied strictly in this litigation, the GDPR would require Ingenico to (a) obtain consent to disclose from every person in the European Union whose personal data (e.g., name, email address, telephone number, job title, or other identifying information) appears in a document; or (b) to the extent consent is not or cannot be obtained, redact all such identifying information.

The GDPR prohibition on processing personal data without consent is subject to certain exceptions. Most relevant here, the GDPR provides that "a transfer or a set of transfer of personal data to a third country or an international organization shall take place only on one of the following conditions: . . . the transfer is necessary for the establishment, exercise or defence of legal claims." (*Id.*, Article 49(1)(e); *see also* Article (18)(1), (2) (permitting processing of personal data "for the establishment, exercise or defence of legal claims" notwithstanding the data subject's objection)).

II. LEGAL STANDARD

"[T]he party seeking to rely on [foreign] law, [has the] burden to demonstrate that these laws bar production of the documents at issue." *Knight Capital Partners Corp. v. Henkel Ag & Co., KGaA*, 290 F. Supp. 3d 681, 689 (E.D. Mich. 2017); *see also Fraunhofer-Gesellschaft zur Forderung der Angewandten Forschung E.V. v. Sirius XM Radio Inc.*, 940 F.3d 1372, 1378 (Fed. Cir. 2019) ("[t]he parties ... generally carry both the burden of raising the issue that foreign law may apply in an action, and the burden of adequately proving foreign law to enable the court to apply it in a particular case."); *Bel-Ray Co. v. Chemrite (Pty) Ltd.*, 181 F.3d 435, 440 (3d Cir. 1999) (same); *United States v. Vetco Inc.*, 691 F.2d 1281, 1289 (9th Cir. 1981) (same); *In re Mercedes-Benz Emissions Litig.*, No. 16-CV-881 (KM) (ESK), 2020 WL 487288, at *6 (D.N.J. Jan. 30, 2020) (same). "[D]istrict courts must be afforded wide latitude in the management of discovery." *Danny B. ex rel. Elliott v. Raimondo*, 784 F.3d 825, 834 (1st Cir. 2015).

III. ARGUMENT

In *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for S. Dist. of Iowa*, the United States Supreme Court observed that "[i]t is well settled that [foreign statutes such as the 'French blocking statute'] do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute." 482 U.S. 522, 544 n.29 (1987). Indeed, the Supreme Court expressed concern that a contrary approach would "effectively subject every American court hearing a case involving a national or a contracting state to the internal laws of that state." *Id.* at 539. Courts are particularly disinclined to apply foreign law where, as here, the foreign party has elected to engage in business in the United States:

> Having elected to establish a major presence in the United States, KPMG–B must have anticipated that it would be subject to suit in this country (and, thus, subject to pretrial discovery rules that are pandemic to the American justice system). *See*

> Restatement (Third) of Foreign Relations Law § 442, reporters' note 1 (1987) (noting "that persons who do business in the United States ... are subject to the burdens as well as the benefits of United States law, including the laws on discovery"). While courts should "take care to demonstrate due respect for any special problem confronted by [a] foreign litigant on account of its nationality," *Société Nationale*, 482 U.S. at 546, 107 S.Ct. 2542, a foreign national that chooses to engage in business in the United States likewise must demonstrate due respect for the operation of the American judicial system

Quaak v. Klynveld Peat Marwick Goerdeler Bedrijfsrevisoren, 361 F.3d 11, 22 (1st Cir. 2004). The international conglomerate Ingenico cannot engage in significant business activity in this country and also reject its discovery rules.

As discussed below, the Court should not apply the GDPR's data protection restrictions to discovery in this case because (1) the Litigation Exemption makes those restrictions inapplicable and (2) notwithstanding the Litigation Exemption, Defendants are unable to prove that the GDPR should apply.

A. The Litigation Exemption Applies

Pursuant to the Litigation Exemption, the GDPR's restrictions on the transfer of personal data do not apply where "the transfer is necessary for the establishment, exercise or defence of legal claims." Interpretation of this provision begins and ends with the plain language of the text:

> When construing a foreign statute, the Court certainly must presume that the most pertinent and authoritative source on the scope and import of any foreign law is the plain language of the statute itself. And any exercise in statutory construction must begin with the plain language of the statute because the language of the statute is the starting point for interpretation, and it should also be the ending point if the plain meaning of that language is clear."

Knight Capital Partners Corp. v. Henkel Ag & Co., KGaA, 290 F. Supp. 3d 681, 687–88 (E.D. Mich. 2017) (citations and internal quotations omitted). Here, a plain reading of the Litigation Exemption shows that the GDPR does not apply: "The plain language of the Act, therefore, suggests that there is no conflict between the discovery obligations under the Federal Rules of

Civil Procedure and any provision of the" GDPR. *Id.*, 290 F. Supp. 3d at 687 (interpreting materially identical litigation exemption under German version of GDPR).

In *Knight Capital*, in the absence of any codified definitions, the court assigned to the terms "necessary" and "legal claims" "their ordinary meanings and construe[d] the statute in accord with its plain language and those ordinary meanings." *Id.* at 688. In interpreting those terms, the court distinguished between discovery seeking "ordinary-course-of-business communications that are typical of the day-to-day business operations of a commercial (i.e., not 'personal') enterprise" and discovery seeking "'personal' data of the disclosing entities" or "intimate, personal details of the defendant's employees." *Id.* at 688. In that regard, the court found that the requested "information concerning the defendant's communications with the plaintiff and third parties about the contemplated technology deal certainly will be 'necessary' to the adjudication of the claims of tortious interference by any sensible construction of the plain language of the statute." *Id.*[2]

The *Knight Capital* analysis is instructive here. During the March 30, 2020 conference, the Court asked counsel for Plaintiffs what types of documents they were seeking and, in particular, whether they would be seeking employee records or personnel files. The answer was no. Rather, as was the case in *Knight Capital*, Plaintiffs are not seeking "personal data" or "intimate, personal details" of Ingenico's employees. Plaintiffs merely seek documents and correspondences relating to their claims for tortious interference, theft of trade secrets, breach of contract, unjust enrichment, and violations of various business statutes – "ordinary-course-of-business [documents] that are typical of the day-to-day business operations" of Ingenico. (*See* Exhibit A).

[2] Courts also have held that disclosure is "necessary" where disclosure has been ordered by the Court. *See, e.g., Royal Park Investments SA/NV v. Deutsche Bank Nat'l Tr. Co.*, No. 14CV04394AJNBCM, 2017 WL 7512815, at *9 (S.D.N.Y. Dec. 29, 2017); *St. Jude Med. S.C., Inc. v. Janssen-Counotte*, 104 F. Supp. 3d 1150, 1163 (D. Or. 2015).

Not only are the requested records the standard types of documents exchanged in discovery, they are necessary for Plaintiffs to develop and prove their claims. As in most cases, the evidence of wrongdoing is in the possession of the defendant(s). This case is no different. Plaintiffs need to be able to discover what Ingenico was doing and saying behind closed doors and with third parties in order to support their claims that Ingenico stole Plaintiffs' trade secrets, tortiously interfered with their contract and business expectancies, and committed other legal violations. In particular, Plaintiffs need to know *who* did what, *who* said what to *whom*, and otherwise *who* the key players are. That would be impossible if Ingenico were permitted to redact all personal data. Accordingly, the requested documents are necessary, and the Litigation Exemption applies. *See also St. Jude Med. S.C., Inc. v. Janssen-Counotte*, 104 F. Supp. 3d 1150, 1163 (D. Or. 2015) (finding that German analog of Litigation Exemption applies); *BrightEdge Techs., Inc. v. Searchmetrics, GmbH.*, No. 14CV01009WHOMEJ, 2014 WL 3965062, at *4 (N.D. Cal. Aug. 13, 2014) (finding that German analog of Litigation Exemption applies "in the case of litigation").

B. The GDPR Should not be Applied to Discovery in this Case.

Even notwithstanding the Litigation Exemption, Defendants still are unable to prove that the GDPR should restrict discovery here. To do so, Defendants would have to show that the following factors weigh in their favor:

1. the importance to the ... litigation of the documents or other information requested;
2. the degree of specificity of the request;
3. whether the information originated in the United States;
4. the availability of alternative means of securing the information; and
5. the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request

> would undermine important interests of the state where the information is located.

Societe Nationale, 482 U.S. at 544 n.28. They do not.

1. The Requested Information is Important.

The requested documents are not only important to developing Plaintiffs' case – they are *the* documents that Plaintiffs need to develop their case. "Where the evidence is directly relevant, [courts have] found this factor to weigh in favor of disclosure." *Finjan, Inc. v. Zscaler, Inc.*, No. 17CV06946JSTKAW, 2019 WL 618554, at *2 (N.D. Cal. Feb. 14, 2019) (quoting *Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468, 1475 (9th Cir. 1992) ("In this case, the information sought is not only relevant to the execution of the judgment, it is crucial")); *see also In re Mercedes-Benz Emissions Litig.*, No. 16-CV-881 (KM) (ESK), 2020 WL 487288, at *6 (D.N.J. Jan. 30, 2020) (finding no need to apply a more heightened standard than "directly relevant").

Plaintiffs claim that Ingenico, among other things, tortiously interfered with Plaintiffs' business relationships and stole their trade secrets. Further, Plaintiffs claim that Ingenico employees based in France were knowledgeable of – and even actively involved with – that wrongful conduct. In order to evaluate that, Plaintiffs must be able to discover who was telling what to whom – especially if those persons were upper level Ingenico employees in France. *See Knight Capital*, 290 F. Supp. 3d at 690 (in case involving claim of tortious interference, requiring disclosure of the defendant's emails "about entering into (or not) an agreement to market products for cleaning oil refinery equipment based on technology owned and to be supplied by [the plaintiff's] technology partner").

Further, to the extent Defendants contend "that the e-mails could be duplicative of production from domestic custodians[, that] argument of duplication is hypothetical," as Defendants have not actually done an email search yet. *Finjan*, 2019 WL 618554, at *2. Nor have

Defendants actually produced any documents to date, further underscoring the importance of the Requests. *See Proofpoint, Inc. v. Vade Secure, Inc.*, No. 19CV04238MMCRMI, 2020 WL 504962, at *2 (N.D. Cal. Jan. 31, 2020) ("Plaintiffs have complained that they have thus far not received any discovery whatsoever, and therefore the court also finds that the discovery presently sought is vital to Plaintiffs' case, and that the requests have been formulated with the requisite degree of specificity in that they are narrowly tailored to target information related to Plaintiffs' misappropriation and breach of contract claims.").

2. The Requested Information is Specific.

Plaintiffs purposefully sought to make their Requests as specific as possible. In preparing the Requests, Plaintiffs dissected each of their claims, scrutinized all of the known facts, evaluated the roles of each of the known players, and picked apart the years-long timeline. That resulted in 126 Requests, all of which specifically targeted and narrowly tailored to their claims. *See Knight Capital*, 290 F. Supp. 3d at 690 (finding that factor weighed In favor of disclosure where "[t]he plaintiff's requests do not demand any substantial mass of unrelated personal information of, for example, employees, customers, or third-party partners of Henkel Global that were uninvolved with the negotiations and the technology discussed in the course of the proposed deal"); *Laydon v. Mizuho Bank, Ltd.*, 183 F. Supp. 3d 409, 421 (S.D.N.Y. 2016) ("plaintiff requests only documents that are important to litigating his claims—i.e., documents that directly relate to whether the Moving Defendants engaged in unlawful manipulation of Yen-LIBOR or Euroyen TIBOR"). Notwithstanding the number of Requests, they are not unduly burdensome or overbroad and do not unnecessarily implicate personal data of persons uninvolved with the issues in this case. *See In re Mercedes-Benz Emissions Litig.*, No. 16-CV-881 (KM) (ESK), 2020 WL 487288, at *7 (D.N.J. Jan. 30, 2020) (finding factor weighed in favor of disclosure notwithstanding "seventy-plus document requests—seeking millions of pages of emails and other documents from numerous

EU citizens"). Tellingly, Defendants did not object on any of those grounds (except as a general objection to the specified relevant time period). (Exhibit C, Defendants' Objections to Plaintiffs' First Set of Requests for Production of Documents; *see also Richmark*, 959 F.2d at 1475 ("In this case, Beijing has not objected to the burdensome nature of the discovery request")). Also, the parties are in the process of negotiating custodians and search terms that will further ensure a refined pool of documents. *See Finjan, Inc.*, 2019 WL 618554, at *2 (finding that targeted search terms weigh in favor of disclosure).

3. The Requested Information is in the United States.

Notwithstanding the involvement of French residents (and their personal data contained in important documents), Plaintiffs expect that much of the documents are in the possession of the U.S.-based Ingenico Defendants – Ingenico Inc. and Ingenico Corp. (*See* Defendants' Answer to the Amended Complaint, ¶¶ 7, 8 (admitting that Ingenico Inc. and Ingenico Corp. are domestic corporations headquartered in Georgia)). This factor weighs in favor of disclosure. *See Proofpoint, Inc. v. Vade Secure, Inc.*, No. 19CV04238MMCRMI, 2020 WL 504962, at *2 (N.D. Cal. Jan. 31, 2020) (finding factor weighed in favor of disclosure where, "[g]iven Defendants[']domestic activities, most of the information sought by the [d]iscovery [r]equests is located in the U.S. and from U.S. entities."); *Finjan*, 2019 WL 618554, at *2 (finding that, where "Defendant itself is an American company, subject to American discovery law[, t]his factor weighs somewhat in favor of disclosure.").

4. There are no Alternative Means of Obtaining the Requested Information.

Defendants cannot show that there exist alternative means of securing the information. "[T]he alternative means must be 'substantially equivalent' to the requested discovery." *Finjan*, 2019 WL 618554, at *2 (quoting *Richmark*, 959 F.2d at 1475). In that sense, redacting all personal

information is not a "substantially equivalent" alternative. *Id.* Nor can Plaintiffs show that limiting production to domestic custodians would serve as a substantially equivalent alternative because (1) they have yet to perform an email search, (2) the location of the documents does not change whether the documents contain personal data of French residents, and (3) as a French company, Ingenico likely would object pursuant to the GDPR whether the documents were in the possession of the French corporate parent or a U.S. affiliate.

5. The Interests of the United States Outweigh the Interests of France.

The United States has an "overriding interest in the just, speedy, and inexpensive determination of litigation in [its] courts," *Societe Nationale*, 482 U.S. at 543, and a "substantial" interest in "vindicating the rights of American plaintiffs," *Richmark*, 959 F.2d at 1477. "The broad right of discovery in American courts is based on the general principle that litigants have a right to every man's evidence, and that wide access to relevant facts serves the integrity and fairness of the judicial process by promoting the search for the truth." *St. Jude*, 104 F. Supp. 3d at 162 (citations and internal quotations omitted). "The interests of the United States in permitting efficient discovery under the Federal Rules are therefore considerable and fundamental." *Id.* "This interest is even stronger where the discovery sought is vital to the litigation." *Laydon*, 183 F. Supp. 3d 409, 423 (S.D.N.Y. 2016).

These interests outweigh foreign countries' interests in privacy, particularly where (a) "the discovery sought . . . is not discovery *of* personal data[, but rather] discovery that *incidentally contains* personal data," *id.* at 1644-45; (b) where a protective order has been entered by the court, *Finjan*, 2019 WL 618554, at *3; *In re Mercedes-Benz Emissions Litig.*, No. 16-CV-881 (KM) (ESK), 2020 WL 487288, at *8 (D.N.J. Jan. 30, 2020) (finding that U.S. "significant interest in preserving and maintaining the integrity of the broad discovery provisions set forth in the Federal Rules of Civil Procedure" outweighs foreign country's privacy interest, particularly "where the

court has entered a protective order preventing disclosure of the secret information"); and (c) "where the [foreign] statute on point expressly allows disclosures that are necessary for the purposes of litigation," *Knight Capital*, 290 F. Supp. 3d at 691. All of those are true here. Plaintiffs do not specifically seek discovery of personal data, though the requested discovery may incidentally contain some; the Court has entered a protective order, which provides sufficient protection for any sensitive or confidential information; and, as discussed above, the Litigation Exemption permits transfer. Accordingly, the interests of the United States outweigh those of France.

In their correspondences with Plaintiffs, Defendants have relied upon an amicus curiae brief submitted by the European Union to the United States Supreme Court in the case of *United States v. Microsoft Corp.* (No. 17-2) that stated that "Article 48 makes clear that a foreign court order does not, as such, make a transfer lawful under the GDPR."[3] That has no bearing on this analysis. Defendants' argument is belied by its own mirror image: just as United States court rulings are not authoritative on foreign law, neither too are foreign authorities binding on United States courts. *Knight Capital*, 290 F. Supp. 3d at 689 ("the defendant's contention that the Court must construe the Data Protection Act by resorting solely to interpretations of German law by German authorities is simply wrong."). Rather, the Court is bound by the law established by the

[3] Article 48 provides that "[a]ny judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter." But that is not what is at issue here. And more importantly, Defendants have waived this argument. In response to Plaintiffs' Requests, Defendants failed to object on ground that the Requests should have been made through the Hague Convention process. Further, during the March 30, 2020 conference, Defendants admitted that they viewed an order from the Court as an appropriate way to resolve this issue. Accordingly, they cannot now argue that the Requests were procedurally improper or that the Court ruling on this issue is nonbinding.

United States Supreme Court and, in particular, its opinion in *Societe Nationale*, where it stated that

> [i]t is well settled that [foreign statutes such as the 'French blocking statute'] do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute. Nor can the enactment of such a statute by a foreign nation require American courts to engraft a rule of first resort onto the Hague Convention, or otherwise to provide the nationals of such a country with a preferred status in our courts. It is clear that American courts are not required to adhere blindly to the directives of such a statute. Indeed, the language of the statute, if taken literally, would appear to represent an extraordinary exercise of legislative jurisdiction by the Republic of France over a United States district judge, forbidding him or her to order any discovery from a party of French nationality . . . .

482 U.S. 522, 544 n.29 (1987) (citations omitted). An EU Commission amicus curiae brief[4] does not dictate the law of the United States.[5]

IV. CONCLUSION

For the foregoing reasons, Plaintiffs request that the Court compel Defendants to produce documents without any redaction or withholding of personal data pursuant to the GDPR.

[4] Defendants have not referred Plaintiffs to any instance where the French government intervened in U.S. litigation with respect to this issue. To the extent intervention by a foreign entity impacts the comity analysis, an amicus curiae brief by the EU Commission does not evidence any interest by *France*. Nor does it evidence the extent to which France enforces the GDPR. *See Finjan*, 2019 WL 618554, at *3 ("the burden of showing that the law bars production is not satisfied where there is no evidence of the extent to which the government enforces its laws"). In fact, courts have observed that "the French Blocking Statute does not subject defendants to a realistic risk of prosecution, and cannot be construed as a law intended to universally govern the conduct of litigation within the jurisdiction of a United States court." *Bodner v. Paribas*, 202 F.R.D. 370, 375 (E.D.N.Y. 2000). Rather, "legislative history of the statute gives strong indications that it was never expected nor intended to be enforced against French subjects but was intended rather to provide them with tactical weapons and bargaining chips in foreign courts." *Compagnie Francaise d'Assurance Pour le Commerce Exterieur v. Phillips Petroleum Co.*, 105 F.R.D. 16, 30 (S.D.N.Y. 1984). There is no indication that the French GDPR is any different.

[5] Notably, the dispute in *United States v. Microsoft Corp.* was rendered moot by the intervening passage of legislation. *See United States v. Microsoft Corp*., 138 S. Ct. 1186, 1188 (2018). The Supreme Court did not refer to the European Union Commission amicus curiae brief in its opinion. *Id.*

Respectfully submitted this 6th day of April, 2020,

/s/ Daniel Carmeli
MELISSA A. BOZEMAN
OLIVER D. GRIFFIN
PETER N. KESSLER
Kutak Rock LLP
1760 Market Street, Suite 1100
Philadelphia, PA 19103
Tel: (215) 288-4384
Fax: (215) 981-0719
Melissa.bozeman@kutakrock.com
Oliver.griffin@kutakrock.com
Peter.kessler@kutakrock.com

DANIEL CARMELI
Kutak Rock LLP
1801 California Street, Suite 3000
Denver, Colorado 80202
Tel: (303) 297-2400
Fax: (303) 292-7799
Daniel.carmeli@kutakrock.com

JONATHON D. FRIEDMANN
ROBERT P. RUDOLPH
Rudolph Friedmann LLP
92 State Street
Boston, MA 02109
Tel: (617) 723-7700
Fax: (617) 227-0313
jfriedmann@rflawyers.com
rrudolph@rflawyers.com

RICARDO G. CEDILLO
Davis, Cedillo & Mendoza, Inc.
755 E. Mulberry Ave., Ste 500
San Antonio, Texas 78212
Tel: (210) 822-6666
Fax: (210) 822-1151
rcedillo@lawdcm.com

Counsel for Plaintiffs AnywhereCommerce, Inc. and BBPOS Limited

CERTIFICATE OF SERVICE

I certify that on this 6th day of April, 2020, the foregoing was electronically filed with the Clerk of Court using the CM/ECF system, which will send notification of such filing to all counsel of record.

/s/ Daniel Carmeli